

Exemplo 2. Distribución Live SystemRescueCD. Acceso mediante SSH ao disco duro dun host arrancado con SystemRescueCD

Exemplo 2. Distribución Live SystemRescueCD. Acceso mediante SSH ao disco duro dun host arrancado con SystemRescueCD

NOTA: Empregando a distribución Live SystemRescueCD podemos acceder por SSH ao disco duro de calquera host (equipo con conexión de rede).

◇ Arrancar SystemRescueCD no host ao cal queremos acceder por SSH á información do seu/s disco/s duro/s:

```
SystemRescueCd
- Linux kernel-2.6.31 (with ext4, reiser4, btrfs filesystems support)
- Both 32bits (IA32) and 64bits (AMD64/EM64T) are supported
- GParted graphical partitioning tool (partition magic clone)
- File systems tools (ext3, ext4, reiserfs, ntfs, btrfs, ...) and LVM2
- Disk tools (parted, sfdisk, partimage, fsarchiver, testdisk, photorec)
- Ntfs-3g (ntfs full read-write support) and ntpass (reset windows passwords)
- Network tools (samba, nfs, ssh, iftop, tcpdump, ...) and wireless drivers
- Network booting via PXE (press F6 for help)

- X.Org / Xfbdev graphical environments with XFCE and Firefox-3.5
- Hardware autodetection and Midnight Commander

==> Press F5 for help if you have boot problems with SystemRescueCd <==

Welcome to SystemRescueCd for x86 (i486+amd64) - version 1.3.5
F2,F3,F4,F5,F6,F7 for boot options and more help.
boot: _
```

```
:: Scanning for firewire::sbp2...
:: Scanning for mdadm::raid0...
:: Scanning for mdadm::raid1...
:: Scanning for mdadm::raid456...
:: Scanning for mdadm::raid10...
>> Performing the network configuration...
>> Activating mdev
>> Making tmpfs for /newroot
>> Attempting to mount media:- /dev/sr0
>> Media found on /dev/sr0
>> Loading keymaps
Please select a keymap from the following list by typing in the
name or number. You should prefer the name to the number (for
type 'fr' instead of '16'). Hit Enter for the default 'us' key
map.

1 azerty 2 be 3 by 4 br-a 5 br-l 6 by
8 croat 9 cz 10 de 11 dk 12 dvorak 13 es
15 fi 16 fr 17 gr 18 hu 19 il 20 is
22 jp 23 la 24 lt 25 mk 26 nl 27 no
29 pt 30 ro 31 ru 32 se 33 sg 34 sk-y
36 slovene 37 trf 38 trq 39 ua 40 uk 41 us
43 fr_CH 44 speakup 45 cs_CZ 46 de_CH 47 sg-lat1 48 fr-be

default choice (US keymap) will be used if no action within 30
s
<< Load keymap (Enter for default): 13_
```

a. Arrancar SystemRescueCD

b. Elixir teclado español (opción 13)

```
* Starting local ... [ ok ]

***** SystemRescue-Cd ----- 1.3.5 ----- tty1/6 ==
http://www.sysrescuecd.org/

- Type net-setup eth0 to specify ethernet configuration.
- If your PC is on an ethernet local network, you can configure by hand:
  - ifconfig eth0 192.168.x.a (your static IP address)
  - route add default gw 192.168.x.b (IP address of the gateway)
- To be sure there is an ssh server running, type /etc/init.d/ssh start.
  You will need to create a user or to change the root password with passwd.
- Available console text editors : nano, vim, gemacs, joe.
- Web browser in the console: elinks www.web-site.org.
- WARNING : Never mount anything on /mnt! It would freeze the system.
  Use mkdir /mnt/mydir and mount on /mnt/mydir instead.
- Ntfs-3g : If you need a full Read-Write NTFS access, use Ntfs-3g.
  Mount the disk: ntfs-3g /dev/sda1 /mnt/windows
- Graphical environment : use either Xorg or Xfbdev.
  Type wizard to run the graphical environment (or startx but it may fail)
  X.Org comes with Window-Maker and you can use several graphical tools:
  - Partition manager:..gparted
  - Web browsers:.....firefox-3.5
  - Text editors:.....gvim and geany

root@sysrescuecd /root % net-setup eth0_
```

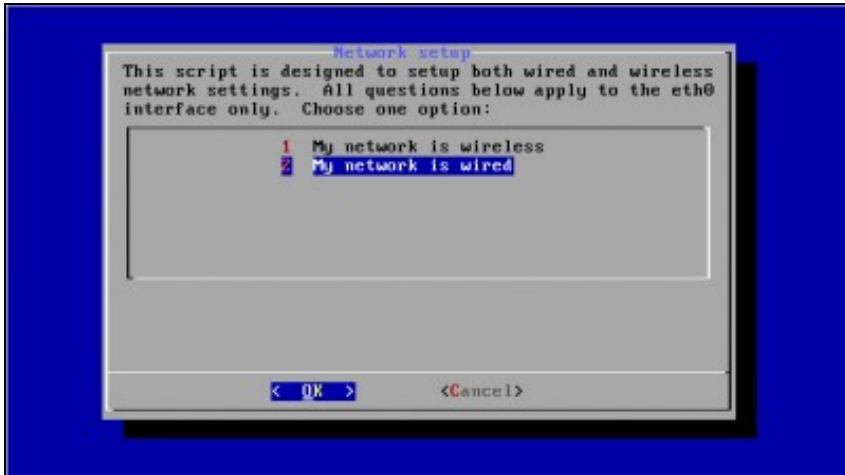
```
Interface details
Details for network interface eth0 are shown below.

Interface name: eth0
MAC address: 00:00:27:74:36:c7
Driver: e1000

Is this the interface that you wish to configure?

[ Yes ] [ No ]
```

c. Configurar a tarxeta de rede eth0



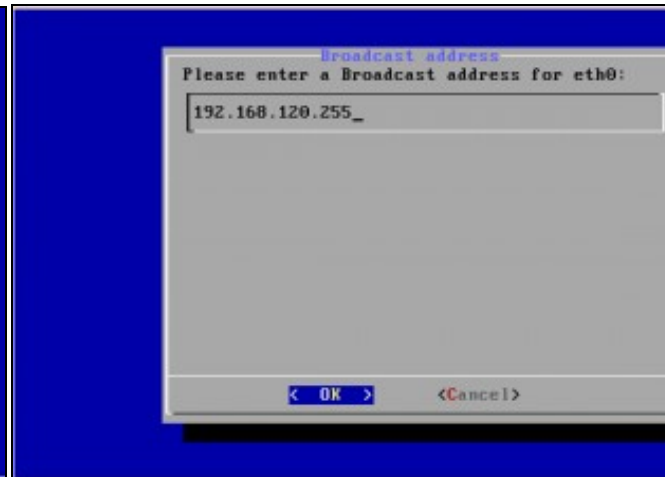
d. Detalles interface eth0



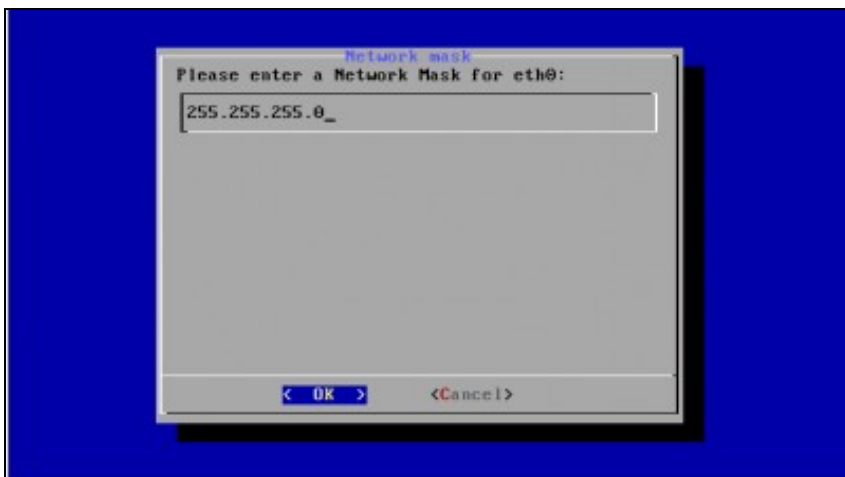
e. Opción 2. Rede cableada



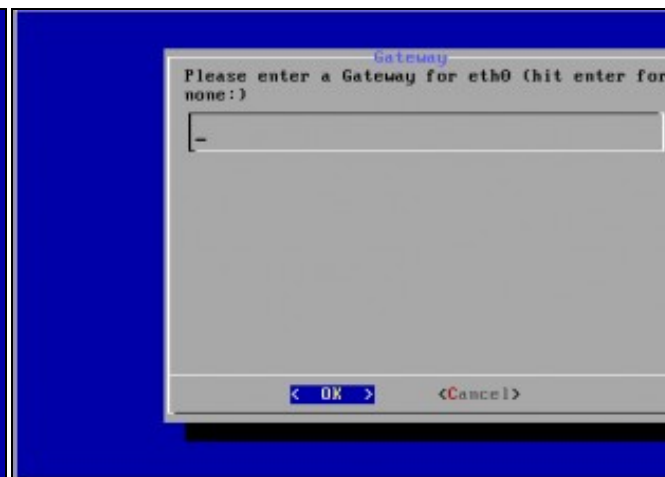
f. Configuración da rede manualmente (NON DHCP)



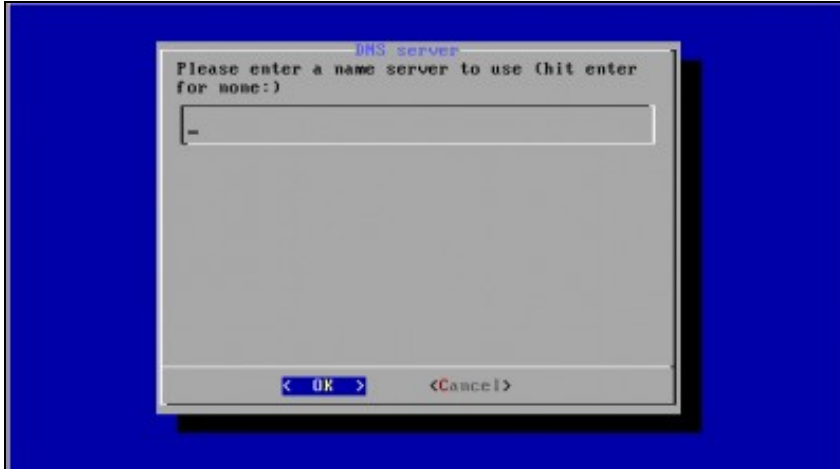
g. IP: 192.168.120.100



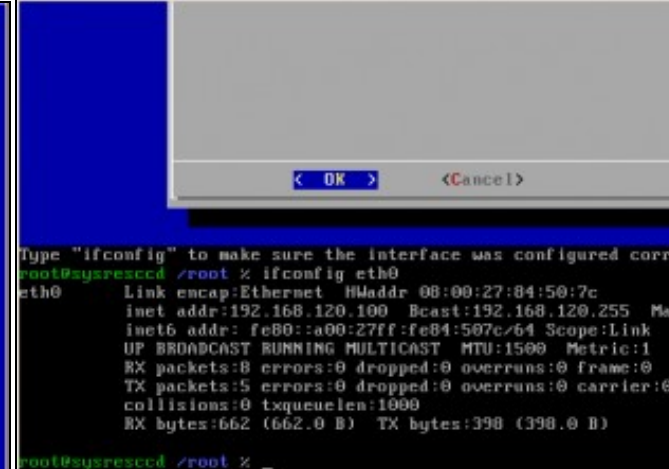
h. Dirección Broadcast: 192.168.120.255



i. Máscara de Subrede: 255.255.255.0



k. Gateway



l. DNS

```
root@sysresccd /root % passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@sysresccd /root % _
```

m. Comprobación configuración rede interface eth0

```
root@sysresccd /root % ssh -v localhost
OpenSSH_5.2p1, OpenSSL 0.9.8l 5 Nov 2009
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Connecting to localhost [127.0.0.1] port 22.
debug1: Connection established.
debug1: permanently_set_uid: 0/0
debug1: identity file /root/.ssh/identity type -1
debug1: identity file /root/.ssh/id_rsa type -1
debug1: identity file /root/.ssh/id_dsa type -1
debug1: Remote protocol version 2.0, remote software version 0
debug1: match: OpenSSH_5.2 pat OpenSSH*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_5.2
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: server->client aes128-ctr hmac-md5 none
debug1: kex: client->server aes128-ctr hmac-md5 none
debug1: SSH2_MSG_KEX_DH_GEX_REQUEST(1024<1024<1024) sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_GROUP
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is 0c:08:12:1e:81:14:3a:df:cb:cc:c5:36:09:b9:38:c8.
Are you sure you want to continue connecting (yes/no)? yes
Are you sure you want to continue connecting (yes/no)? yes
```

n. Password root: toor

```
debug1: expecting SSH2_MSG_KEX_DH_GEX_GROUP
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is 0c:08:12:1e:81:14:3a:df:cb:cc:c5:36:09:b9:38:c8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
debug1: ssh_rsa_verify: signature correct
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,keyboard-interactive
debug1: Next authentication method: publickey
debug1: Trying private key: /root/.ssh/identity
debug1: Trying private key: /root/.ssh/id_rsa
debug1: Trying private key: /root/.ssh/id_dsa
debug1: Next authentication method: keyboard-interactive
Password:
debug1: Authentication succeeded (keyboard-interactive).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
root@sysresccd /root % _
```

ñ. Comprobación funcionamiento ssh

Mediante o comando `ssh -v localhost` comprobamos se o servidor S podemos conectarnos a el dende `localhost`. Como é a primeira ver q o servidor avísanos se estamos de acordo coa autenticación. Respos

o. Continuación comprobación funcionamiento ssh... Servidor SSH funcionando.

Conexión mediante o cliente liña de comandos ssh

NOTA: Considérase que o servidor SSH da distribución Live CD ten a configuración por defecto: Porto 22, Permisos de Conexión para root e Non Redireccionamento X.

Acceder a un terminal Linux e proceder como se comenta nas seguintes imaxes:

```
ubuntu@ubuntu: ~  
Archivo Editar Ver Terminal Ayuda  
ubuntu@ubuntu:~$ ifconfig -a  
eth0      Link encap:Ethernet direcciónHW 08:00:27:df:14:f2  
          Direc. inet:10.0.2.15 Difus.:10.0.2.255 Másc:255.255.255.0  
          Dirección inet6: fe80::a00:27ff:fedf:14f2/64 Alcance:Enlace  
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1  
          Paquetes RX:28 errores:0 perdidos:0 overruns:0 frame:0  
          Paquetes TX:64 errores:0 perdidos:0 overruns:0 carrier:0  
          colisiones:0 long.colaTX:1000  
          Bytes RX:8195 (8.1 KB) TX bytes:7820 (7.8 KB)  
          Interrupción:11 Dirección base: 0xd020  
  
lo        Link encap:Bucle local  
          Direc. inet:127.0.0.1 Másc:255.0.0.0  
          Dirección inet6: ::1/128 Alcance:Anfitrión  
          ACTIVO LOOPBACK FUNCIONANDO MTU:16436 Métrica:1  
          Paquetes RX:4 errores:0 perdidos:0 overruns:0 frame:0  
          Paquetes TX:4 errores:0 perdidos:0 overruns:0 carrier:0  
          colisiones:0 long.colaTX:0  
          Bytes RX:240 (240.0 B) TX bytes:240 (240.0 B)  
  
ubuntu@ubuntu:~$
```

a. Executamos o comando `ifconfig -a` para ver todas as tarxetas de rede conectadas a este equipo.

Neste caso a tarxeta de rede que nos interesa é a **eth0**

```
ubuntu@ubuntu: ~  
Archivo Editar Ver Terminal Ayuda  
ubuntu@ubuntu:~$ sudo ifconfig eth0 192.168.120.101/24  
ubuntu@ubuntu:~$ ping -c2 192.168.120.100  
PING 192.168.120.100 (192.168.120.100) 56(84) bytes of data.  
64 bytes from 192.168.120.100: icmp_seq=1 ttl=64 time=5.69 ms  
64 bytes from 192.168.120.100: icmp_seq=2 ttl=64 time=0.886 ms  
  
--- 192.168.120.100 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 0.886/3.291/5.696/2.405 ms  
ubuntu@ubuntu:~$
```

b. Configuramos a tarxeta de rede **eth0**:

IP/MS: 192.168.120.101/24.

Executar no terminal o comando:

`sudo ifconfig eth0 192.168.120.1/24` se o usuario co que traballamos é **root**

ou

`ifconfig eth0 192.168.120.1/24` se somos o usuario **root**

A continuación co comando `ping -c2 192.168.120.100` comprobamos a conexión co **Servidor SSH** enviando dous paquetes do comando `ping`

```
ubuntu@ubuntu: ~  
Archivo Editar Ver Terminal Ayuda  
ubuntu@ubuntu:~$ ssh root@192.168.120.100  
The authenticity of host '192.168.120.100 (192.168.120.100)' can't be established.  
RSA key fingerprint is 69:2e:df:1d:63:b2:42:78:9b:60:37:f5:86:05:95:83.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.120.100' (RSA) to the list of known hosts.  
Password:  
Last login: Mon Apr 19 20:35:15 UTC 2010 from 192.168.120.101 on pts/0  
root@sysresccd /root %
```

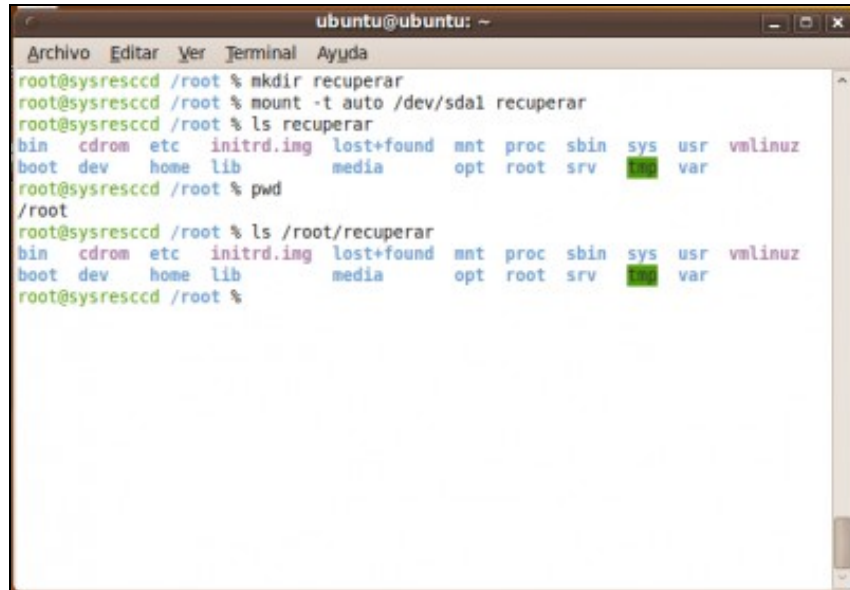
```
ubuntu@ubuntu: ~  
Archivo Editar Ver Terminal Ayuda  
root@sysresccd /root % fdisk -l  
  
Disk /dev/sda: 4294 MB, 4294967296 bytes  
255 heads, 63 sectors/track, 522 cylinders  
Units = cylinders of 16065 * 512 = 8225280 bytes  
Disk identifier: 0x000b7eb9  
  
   Device Boot      Start         End      Blocks   Id  System  
   /dev/sda1  *          1         492     3951958+   83  Linux  
   /dev/sda2             493         522       240975    5  Extended  
   /dev/sda5             493         522       240943+   82  Linux sw  
root@sysresccd /root %
```


c. Conexión co Servidor SSH.

Executamos o comando **ssh root@192.168.120.100**. Como é a primeira vez que nos conectamos o servidor avísanos se estamos de acordo coa autenticación. Respostamos **yes**.

toor é a password pedida de **root**.

Conexión establecida.



```
ubuntu@ubuntu: ~
Archivo  Editar  Ver  Terminal  Ayuda
root@sysresccd /root % mkdir recuperar
root@sysresccd /root % mount -t auto /dev/sda1 recuperar
root@sysresccd /root % ls recuperar
bin  cdrom  etc  initrd.img  lost+found  mnt  proc  sbin  sys  usr  vmlinuz
boot  dev  home  lib  media  opt  root  srv  tmp  var
root@sysresccd /root % pwd
/root
root@sysresccd /root % ls /root/recuperar
bin  cdrom  etc  initrd.img  lost+found  mnt  proc  sbin  sys  usr  vmlinuz
boot  dev  home  lib  media  opt  root  srv  tmp  var
root@sysresccd /root %
```

d. Ver a táboa de particións do equipo (fdisk -l).

Neste caso o equipo posúe o disco duro **/dev/sda**

e. Crear cartafol para acceder á información do disco duro /dev/sda

No cartafol creado, en **/root**, mediante o comando **mkdir recuperar** montamos a partición do disco **/dev/sda** co comando:

mount -t auto /dev/sda1 recuperar

Co comando **ls recuperar** revisamos o contido do cartafol **recuperar**.

NOTA: A ruta completa do cartafol **recuperar** creado é **/root/recuperar**

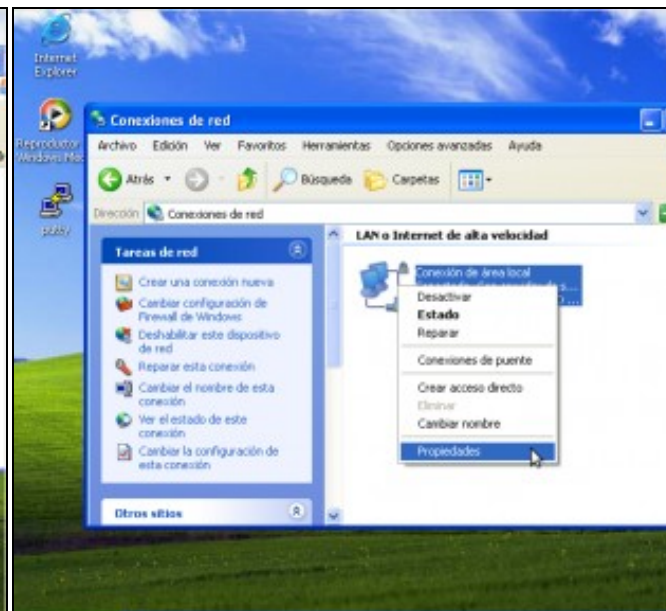
Conexión mediante o cliente gráfico putty para plataformas Windows e UNIX

NOTA: Considérase que o servidor SSH da distribución Live CD ten a configuración por defecto: Porto 22, Permisos de Conexión para root e Non Redireccionamento X.

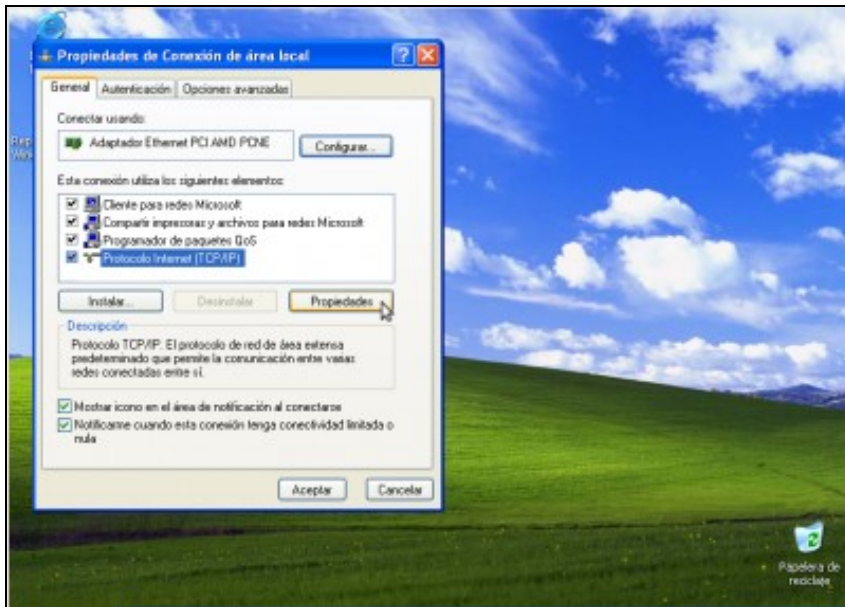
Acceder a un equipo Windows co programa **putty** e proceder como se comenta nas seguintes imaxes:



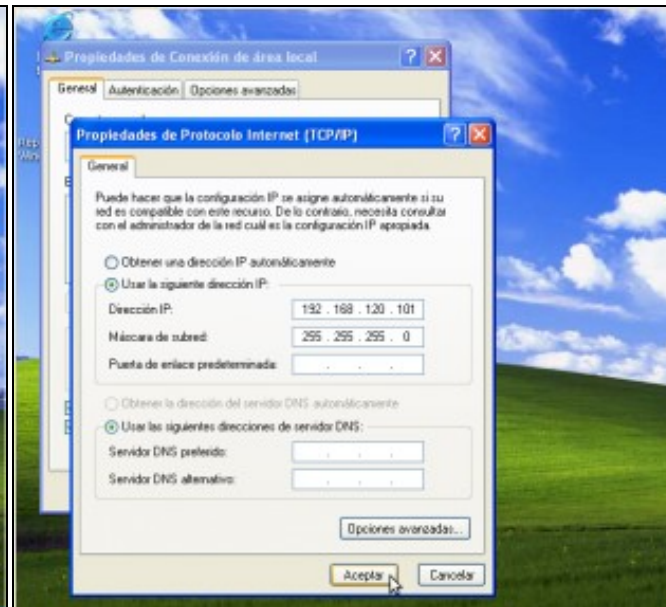
a. Panel de Control-->Conexiones de Red.



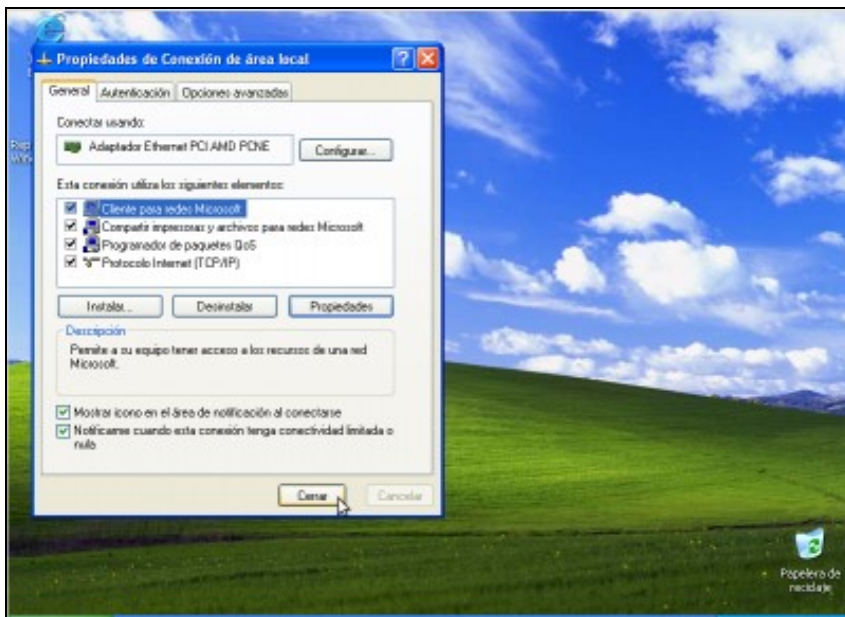
b. Conexión de Área Local-->Propiedades.



c. Protocolo Internet TCP/IP-->Propiedades.



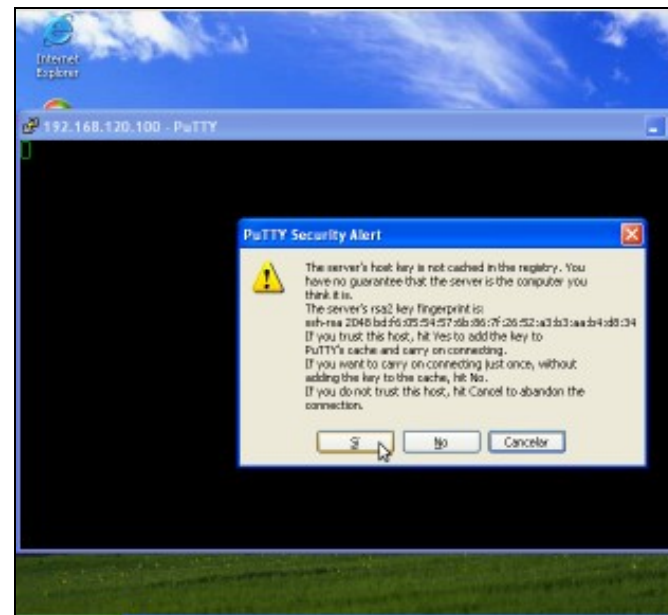
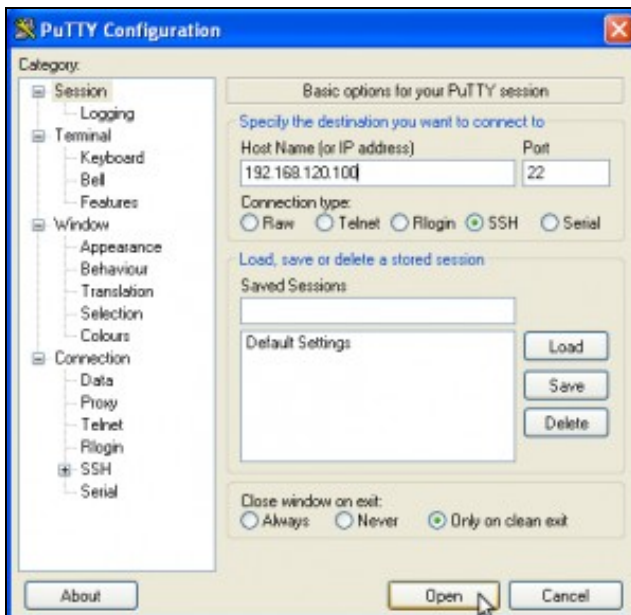
d. IP/MS: 192.168.120.101/255.255.255.0



e. Picar en cerrar para guardar a configuración

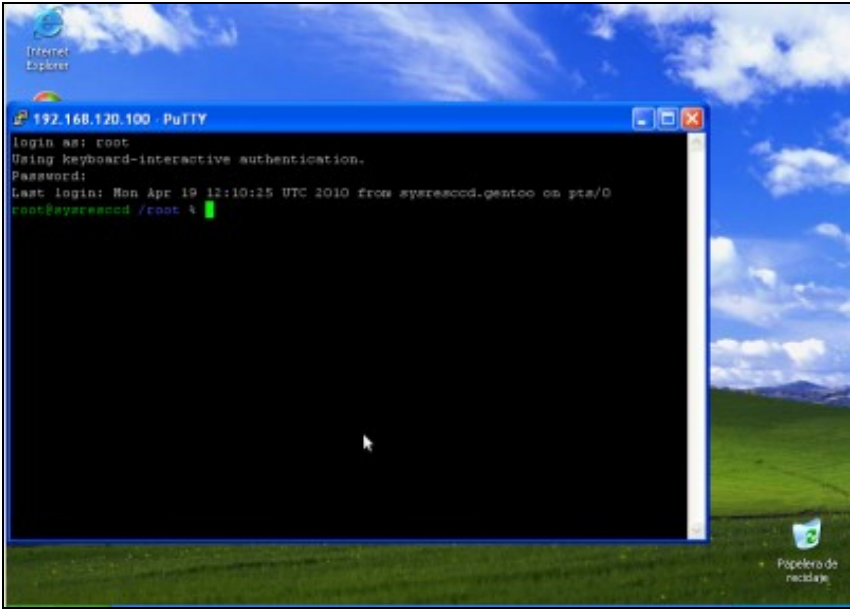


f. Dobre click na icona do escritorio putty para lanzar putty

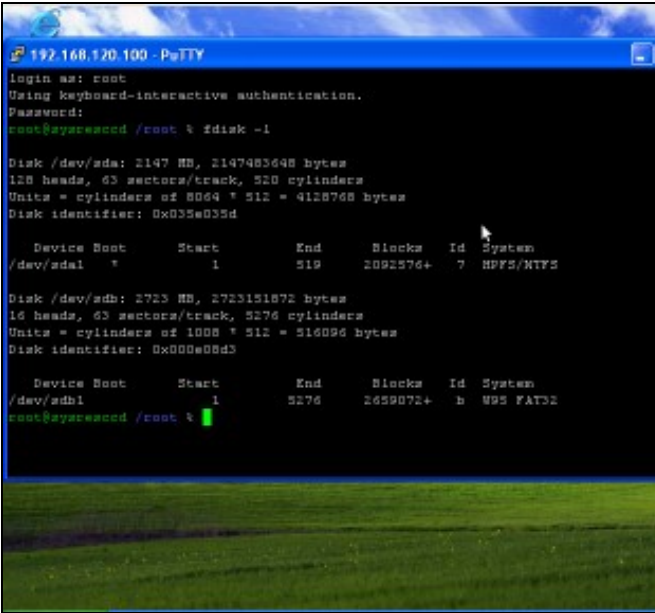


h. Conectando... Como é a primeira vez que nos conectamos o serv
estamos de acordo coa autenticación. Prememos en **Sí**.

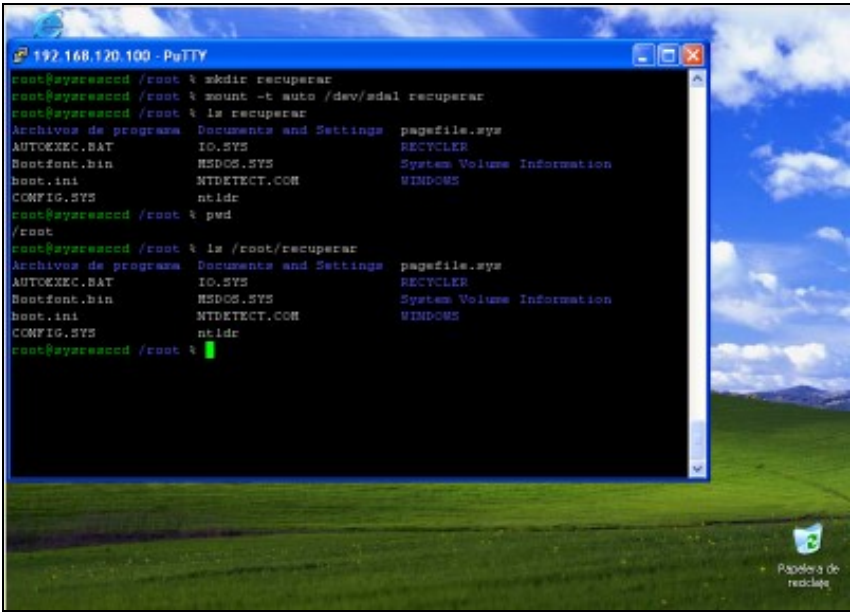
g. Simplemente temos que por a dirección **IP** ou **Host Name** do servidor **SSH** e picar en **Open**. A conexión establecerase no **Porto** por defecto para a conexión **SSH**: o porto **22**



i. **Petición de login e password.** Establecemos a conexión co usuario **root**, coa password **toor** , que modificamos anteriormente.
Conexión establecida. Agora xa temos unha consola remota da distribución **SystemRescueCD** mediante unha conexión **SSH**



k. **Ver a táboa de particións do equipo (fdisk -l).**
Neste caso o equipo posúe 2 discos duros **/dev/sda** e **/dev/sdb**



I. Crear cartafol para acceder á información do disco duro /dev/sda

No cartafol creado, en **/root**, mediante o comando ***mkdir recuperar*** montamos a partición do disco **/dev/sda** co comando:

mount -t auto /dev/sda1 recuperar

Co comando ***ls recuperar*** revisamos o contido do cartafol **recuperar**.

NOTA: A ruta completa do cartafol recuperar creado é /root/recuperar

--ricardofc [27/04/10]